Manuel d'utilisation du switch HyperDSL

- Branchement du switch et mise à la terre.....2
- Première installation et configuration globale.....3
- Configuration des VLANs.....8
- Régler la priorité des flux de données.....12

BRANCHEMENT DU SWITCH ET MISE À LA TERRE

Ne pas perdre de vue que le switch est connecté à de la radio et est situé sur des sites fortement pollués par des champs radio multiples et puissants. Le non respect des consignes ci-dessous provoque des dysfonctionnements et entraîne la perte de la garantie des équipements.

Le Switch HyperDSL et son alimentation doivent être installés **OBLIGATOIREMENT** sur un rail DIN normalisé afin d'assurer convenablement leur ventilation passive par convection de bas en haut. En aucun cas ne les laisser poser à même le sol, sur une tablette ou sur une étagère.

Etapes du montage :

1. Installez un rail DIN dans une baie ou sur une paroi avec un déport suffisant.

2. Raccorder ce rail DIN à la masse de la baie raccordée à une terre conforme ou à une terre autre que celle de la distribution électrique.

3. Positionnez le switch et son alimentation 220/48VDC sur le rail DIN. Les modules doivent-être espacés d'au moins **2 cm**. **Les blindages ne doivent pas se toucher** pour des aspects thermiques et électriques évidents.

4. Raccordez la connection terre de l'alimentation à la connection terre du switch via le plot à vis de l'alimentation repéré ⏚ via un câble souple (jaune vert) de 1,5mm et une cosse à sertir à l'aide de la vis cuivre ⏚ prévue à cet effet à l'arrière du switch.

5. Raccordez le plot de sortie 48VDC de l'alimentation et le plot d'alimentation 48VDC du switch à l'aide d' une paire torsadée constituée de 2 fils de 1,5mm, repérée Rouge + 48VDC et Bleu – 48VDC. Cette paire torsadée sera en outre, avant le raccordement, enroulée en spirale à l'aide d'un mandrin (axe de tournevis par exemple) en 6 à 8 spires jointives.

Notez que ces précautions sont indispensables afin d'assurer la protection du switch et de son alimentation et d'éviter les interférences radio et les inductions radioélectriques parasites; la torsade du câble 48VDC annulant les effets induits.

6. Vérifiez que les étapes 1.à 5. sont correctes et qu'il n'y a aucune inversion de polarité ou erreur de câblage.

7. Connectez la prise secteur d'alimentation électrique avec deux fils seulement, en respectant **IMPERATIVEMENT** le neutre et la phase. Pour mémoire les cordons moulés normalisés deux fils disposent pour le neutre d'un fil bleu et pour la phase d'un fil marron.

8. Avant raccordement à la prise secteur ou au commutateur de distribution électrique, vérifiez que le neutre correspond bien au neutre en mesurant simplement la tension électrique entre le Neutre et la Terre ⏚. Vous ne devez trouver aucune tension, ou une tension très faible.

Au niveau de l'alimentation 220 AC/48 VDC, ne jamais raccorder la terre du réseau de distribution électrique (jaune vert de la prise secteur) à la terre ou masse de la baie du rail DIN et du switch: celà provoquerait une boucle de courant dangereuse. L'équipotentialité est déjà traitée en amont dans l'installation électrique elle même.

PREMIÈRE INSTALLATION ET CONFIGURATION GLOBALE

Lors de la première installation du switch (configuration sortie d'usine), il faut veiller à lui attribuer une adresse IP.

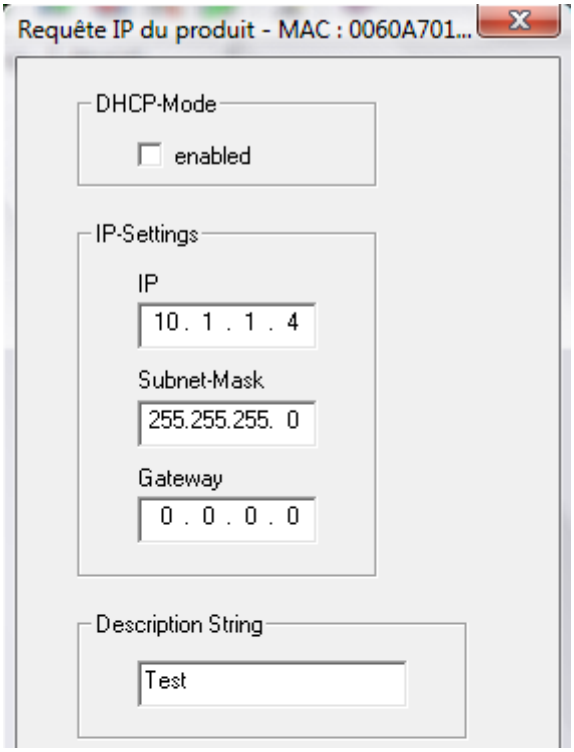
1. Installez le logiciel Device Manager et exécutez l'application via le raccourcie présent sur le bureau.

L'utilisateur par défaut est **admin** sans mot de passe.

2. Connectez-vous physiquement au switch en utilisant un câble droit ou croisé sur le port 2 (le 1 étant réservé pour une autre utilisation).

3. Après avoir désactivé votre pare-feu, appuyez 2 secondes sur le **bouton non repéré** en haut à gauche afin de lancer une demande d'adresse IP par le switch (broadcast).

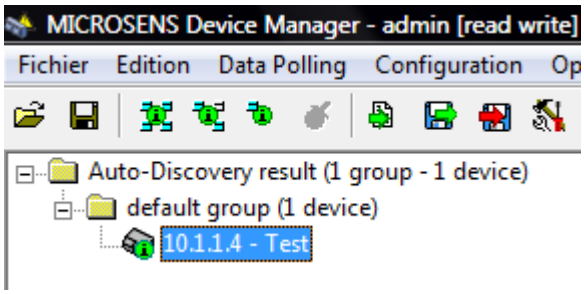
4. Attribuez une IP dans la classe d'adresse privée **10.1.1.0** (masque de sous réseau: **255.255.255.0**) au switch ainsi qu'un nom. Cliquez sur Send pour appliquer la configuration.



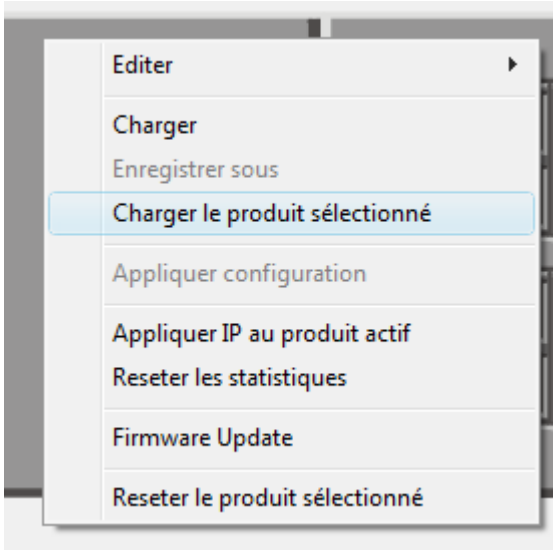
5. Modifiez l'adresse IP de votre ordinateur pour être dans le même réseau que celui du switch (c'est-à-dire **10.1.1.0** avec le bon masque **255.255.255.0**). Utilisez 10.1.1.100 par exemple.

Maintenant que votre switch est identifié sur le réseau, nous pouvons commencer à modifier sa configuration globale soit par le logiciel Device Manager, soit par l'interface web du switch.

- Si vous souhaitez utilisez le logiciel, faîtes une **auto-détection** en appuyant sur F8 ou en cliquant sur l'icône . Le switch doit apparaître dans le menu de gauche:



Il faut ensuite charger la configuration initiale du switch. Pour cela faîtes un clique droit dans le cadre de droite et sélectionner « **Charger le produit sélectionné** »



- Si vous souhaitez utilisez l'interface web, connectez-vous en utilisant l'adresse **http://IP_du_switch** (http://10.1.1.1 dans notre exemple). Utilisez le mot de passe admin pour vous connecter en tant que tel.

Le switch permet une configuration en profondeur via l'interface web. Certaines fonctionnalités sont présentes dans cette interface mais pas dans l'application Device Manager. Cette dernière permet cependant de charger et d'enregistrer une configuration de base.

J'utiliserai l'interface web pour illustrer la configuration du switch, mais il est possible d'obtenir l'équivalent en faisant clique droit: **Editer >** … dans l'application Device Manager de Microsens. N'oubliez pas ensuite d'appliquer votre configuration en faisant clique droit: **Appliquer configuration.**

1. Dans le menu « **Port Settings** » de l'interface web (ou la **configuration Hardware** dans le Device Manager), vous pouvez configurez les ports de 1 à 10. Les ports 9 et 10 sont utilisés dans le cas de l'anneau optique.

Port settings

Port	Alias	enabled	Autoneg.	Speed	Duplex	Flow control	MDI/MDIX	FEF
1 (TP/SFP)	Port 1	☑	☑ enable	10MBit 100MBit 1GBit	HDX FDX	advertise avoid	Auto ☑ MDI MDIX	-
2 (TP)	Port 2	☑	☑ enable	10MBit 100MBit	HDX FDX	advertise avoid	Auto ☑ MDI MDIX	-
3 (TP)	Port 3	☑	☑ enable	10MBit 100MBit	HDX FDX	advertise avoid	Auto ☑ MDI MDIX	-
4 (TP)	Port 4	☑	☑ enable	10MBit 100MBit	HDX FDX	advertise avoid	Auto ☑ MDI MDIX	-
5 (TP)	Port 5	☑	☑ enable	10MBit 100MBit	HDX FDX	advertise avoid	Auto ☑ MDI MDIX	-
6 (TP)	Port 6	☑	☑ enable	10MBit 100MBit	HDX FDX	advertise avoid	Auto ☑ MDI MDIX	-
7 (TP)	Port 7	☑	☑ enable	10MBit 100MBit	HDX FDX	advertise avoid	Auto ☑ MDI MDIX	-
8 (TP)	Port 8	☑	☑ enable	10MBit 100MBit	HDX FDX	advertise avoid	Auto ☑ MDI MDIX	-
9 (SFP)	Port 9	☑	☑ enable	100MBit 1GBit	HDX FDX	advertise avoid	-	☐ FEF
10 (SFP)	Port 10	☑	☑ enable	100MBit 1GBit	HDX FDX	advertise avoid	-	☐ FEF

Le FEF (Far End Fault) est un mécanisme permettant de notifier la rupture d'une liaison aux équipements dans le cadre de l'anneau optique. La configuration par défaut est tout à fait satisfaisante.

2. Le menu Ring permet la configuration du switch quand celui-ci est présent dans l'anneau optique.

Ring Settings

Enable Mode	☐
Configuration	Master Slave
Ring Number	1

Chaque anneau ne possède qu'un seul master.

3. Dans le menu « **IGMP-Snooping** » (permettant de gérer les paquets multicast), pensez à cocher « **Flooding Unregister Packet enabled** » et « **IGMP Snooping Enabled** ». Cela permettra de limiter le broadcast des paquets multicast connus transmis sur le réseau, et d'émettre en broadcast ceux qui sont inconnus.

Basic Configuration	
IGMP Snooping enabled	☑
Fast Leave Enabled	☐
Report Aggregation enabled	☐
Flooding Unregister Packet enabled	☑
Group Limit	32
Multicast Router Detection	○ Multicast Router Discovery ◉ by Query Message

Port Configuration	
IGMP Snooping enabled	1: ☑ 2: ☑ 3: ☑ 4: ☑ 5: ☑ 6: ☑ 7: ☑ 8: ☑ 9: ☑ 10: ☑
Static Router Ports	1: ☐ 2: ☐ 3: ☐ 4: ☐ 5: ☐ 6: ☐ 7: ☐ 8: ☐ 9: ☐ 10: ☐

Timeout Variables Configuration	
Multicast Group Configuration	
Group Membership Interval (sec.)	260
Maximum Response Time (sec.)	20
Last Member Query Time (sec.)	2
Multicast Router Configuration	
By MRD: NeighborDeadInterval (sec.)	62
By Query: Router Aging Time (sec.)	260

4. La configuration de la POE (Power Over Ethernet) se fait via la section **PoE Settings**. N'utilisez que le mode d'auto-négociation (802.3af).

Basic Settings	
Total Input Power (W)	65
Switch Supply Power (W)	8
Available PoE-Power (W)	57
Current PoE Power (W)	0

Port Settings

Port-No.	PoE Mode	PoE Status	permitted Power (W)	measured Power (W)	maximum PD class	detected PD class
Port 1	disabled	disabled	15.4	0.0	0: max. 15.4 W	unknown
Port 2	disabled	disabled	15.4	0.0	0: max. 15.4 W	unknown
Port 3	disabled	disabled	15.4	0.0	0: max. 15.4 W	unknown
Port 4	disabled	disabled	15.4	0.0	0: max. 15.4 W	unknown
Port 5	802.3af	disabled	15.4	0.0	0: max. 15.4 W	unknown
Port 6	802.3af	disabled	15.4	0.0	0: max. 15.4 W	unknown
Port 7	802.3af	disabled	15.4	0.0	0: max. 15.4 W	unknown
Port 8	802.3af	disabled	15.4	0.0	0: max. 15.4 W	unknown

Hint: The sum of the permitted power ratings exceeds the available PoE-power.

*Lors de l'activation de la POE sur certains ports, ne faîtes pas attention au message rouge. Il ne faut y faire attention que lorsque la PoE est activé sur plus de 4 ports: le switch ne pourra délivrer 15.4W sur les 5 ports étant donné que la limite est fixé à 65W (15,4*5 = 77 > 65).*

Ici, nous n'activons la PoE que sur les 4 derniers ports.

5. La partie **Admin** contient une section permettant la remise par défaut de la configuration du switch, la mise à jour du firmware et la modification des mots de passe pour l'accès à l'interface web.

Password-Setting		
Userlevel	new Password	retype new Password
Public		
User		
Administrator		

CONFIGURATION DES VLANS

La configuration des VLAN peut se faire via l'interface web (dans la section **VLAN Settings**) ou le Device Manager (clique droit: **Editer > Options de configuration VLAN**).

ATTENTION: *La configuration des VLANs doit se fait obligatoirement lorsque les équipements sont connectés aux ports du switch auxquels vous attribuerez la configuration. Sinon, lorsque vous brancherez l'appareil, vous n'observerez aucun trafic.*

Le switch permet différent modes de fonctionnement pour les ports attachés aux VLANs:

- **Access**: On ajoute aux paquets de possédant pas de tag (ie absence de VlanID dans l'en-tête Ethernet – norme 802.1Q) un tag permettant d'identifier le VLAN sur lequel il se trouve (en suivant l'attribution du **Default-VID** du port dans la configuration). Les paquets sont ensuite filtrés. Les paquets possédant déjà le tag, sont uniquement filtrés (pas de modification du tag). Les paquets sortants (en direction des terminaux) sont détaguées.

- **Trunk**: Les paquets ne sont pas manipulés au niveau de leur tag. Ils sont uniquement filtrés, même s'ils ne possèdent pas de tag.

- **Hybrid**: Similaire au mode Access, mais les paquets sortant ne sont pas détaguées.

Lors de l'attribution de ces différents modes de fonctionnement, il faut bien faire attention que certains équipements ne comprennent pas le tag du VLAN présent dans l'en-tête Ethernet. Ils ne répondront donc à aucune requête car le paquet reçu leur est incompréhensible (utiliser le mode Access dans ce cas).

Il est aussi possible de configurer un VLAN spécial pour accéder au management du switch. Cette fonction accroit la sécurité en restreignant l'accès à l'administration du switch.

1er exemple de configuration des VLANs:

Séparer les données venant du réseaux Ethernet et les données venant d'un lien radio Mobirake sur le port 2 (les débits sont différents). Le port 1 (Gigabit FD) sert à l'upload et est connecté aux autres switchs dans le cas d'une topologie en étoile. Le port de management du switch est lui aussi restreint à un VLAN spécial accessible uniquement depuis un port.

Basic Settings	
VLAN Filter enabled	☑
Force Default VID	☐

Port-No.	VLAN-Mode	Default-VID	Default-Priority
Port 1	Trunk	1	0
Port 2	Access	2	0
Port 3	Access	1	0
Port 4	Access	1	0
Port 5	Access	1	0
Port 6	Access	1	0
Port 7	Access	1	0
Port 8	Access	1	0
Port 9	Access	1	0
Port 10	Access	1	0
Manager	Access	100	7

VLAN Filter

No.	enabled	Alias	VlanID	1	2	3	4	5	6	7	8	9	10	M
1	☑	Data	1	☑	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑
2	☑	Radio	2	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☑	Administration	100	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☑
4	☐	Vlan filter 4	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	Vlan filter 5	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	Vlan filter 6	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	Vlan filter 7	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	Vlan filter 8	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	Vlan filter 9	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	Vlan filter 10	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
11	☐	Vlan filter 11	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
12	☐	Vlan filter 12	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
13	☐	Vlan filter 13	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	☐	Vlan filter 14	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
15	☐	Vlan filter 15	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
16	☐	Vlan filter 16	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

*Bien penser à cocher l'option « **VLAN Filter enabled** », sinon toute la configuration entrée ne sera pas effective.*

Le port 1 étant connecté aux autres équipements du réseau, il ne doit pas enlever le tag VLAN des paquets et doit se charger uniquement de filtrer les paquets et de les acheminer. Il est donc en mode Trunk.

En mode Trunk, le Default-VID est inutile.

Ainsi, tous les ports de 3 à 10 ont accès au port 1 d'upload et au reste du réseau. Le port 8, quant à lui, a aussi accès à l'administration du switch. Il faut bien noter qu'il est impossible d'y accéder depuis un autre port. On aurait pu ajouter dans la table le port 1 comme faisant parti du VLAN 100, afin d'accéder au management depuis un autre emplacement dans le réseau (emplacement faisant parti du VLAN 100).

*Dans le cas d'une mauvaise configuration de VLANs, notamment celui du management et qu'il vous devient impossible d'y accéder, il faudra réinitialiser le switch avec ses paramètres par défaut de sortie d'usine. Pour cela, appuyer simultanément sur les deux boutons (**non identifié** et **Reset**) pendant 10 secondes. Toute la configuration (sauf l'IP et le nom) sera effacé.*

La premier tableau (**Port-No**) permet d'attribuer un VLAN-ID (VID) aux paquets entrants (en direction du switch et du reste du réseau) en mode Access et Hybrid: **Default-VID**. La priorité, Default-Priority (priorité des paquets Ethernet - norme 802.1P) sera traitée dans la section suivante.

Le deuxième tableau (**VLAN Filter**) réalise le filtrage en suivant le VID et le numéro de port. Par exemple, le VID attribué aux paquets venant du port 2 est 2. En lisant le tableau, à la deuxième ligne (VlanID = 2), on se rend compte que le port 2 n'a accès qu'au port 1. Les données venant de ce port ne pourront donc pas perturber celle venant d'autres ports et inversement. Ceci est très pratique dans le cas de diffusion (broadcast) de message n'étant pas adressé au Mobirake. Le port 2 ne sera donc accessible que depuis le VLAN 100.

Concernant le port 8, on remarque que son VID est 1 et qu'il a accès au port de

management en plus du reste du réseau. Ceci est possible car les données sortant du port 8 appartiennent au VLAN 1, comme le port de management (il est coché sur le VLAN Data). Cependant, les données venant du port de management appartiennent au VLAN 100, et uniquement le port 8 appartient aussi au VLAN 100. D'où le fait que le management ne soit pas accessible depuis un autre port.

Un port peut appartenir à plusieurs VLANs (exemple du port 8), mais les données en provenance d'un port appartiendront toujours à un, et un seul VLAN.

2ème exemple de configuration des VLANs:

Récupération des données en provenance du Mobirake (VLAN 2). Le switch utilise maintenant les ports 9 et 10 pour l'upload (exemple: l'anneau optique).

Basic Settings	
VLAN Filter enabled	☑
Force Default VID	☐

Port-No.	VLAN-Mode	Default-VID	Default-Priority
Port 1	Access	1	0
Port 2	Access	1	0
Port 3	Access	1	0
Port 4	Access	1	0
Port 5	Access	1	0
Port 6	Access	1	0
Port 7	Access	1	0
Port 8	Access	1	0
Port 9	Trunk	1	0
Port 10	Trunk	1	0
Manager	Access	100	7

VLAN Filter

No.	enabled	Alias	VlanID	1	2	3	4	5	6	7	8	9	10	M
1	☑	Data	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐
2	☑	Radio	2	☐	☐	☐	☐	☑	☐	☐	☐	☑	☑	☐
3	☑	Administration	100	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☑
4	☐	Vlan filter 4	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	Vlan filter 5	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	Vlan filter 6	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	Vlan filter 7	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	Vlan filter 8	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	Vlan filter 9	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	Vlan filter 10	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
11	☐	Vlan filter 11	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
12	☐	Vlan filter 12	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
13	☐	Vlan filter 13	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	☐	Vlan filter 14	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
15	☐	Vlan filter 15	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
16	☐	Vlan filter 16	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Les ports 9 et 10 sont configurés en mode Trunk pour laisser passer tous les VLANs.

Concernant l'administration, le schéma est différent que dans le premier exemple: l'accès à l'administration ne peut se faire que depuis l'extérieur et depuis le VLAN 100. Cela accroit la sécurité car l'accès au port de management est impossible depuis le VLAN 1. Pour l'accroître d'avantage, il suffirait de modifier le Default-VID du port 8 à 100 (sans oublier de l'inclure dans le VLAN), et de bloquer l'accès au port de management depuis les ports 9 et 10.

Les ports 1 à 8 ont tous accès au reste du réseau. Le point particulier à noter est celui du port 5 qui appartient au VLAN 2 (la radio). Il pourra donc recevoir les informations émises par le Mobirake, mais ne pourra pas lui répondre (nous supposons que le flux vidéo en provenance du Mobirake est unidirectionnel). Ceci est vrai car le port 5 appartient au VLAN 2, mais que les données en provenance du port 5 appartiennent au VLAN 1 (voir la note précédente).

Si nous voulons autoriser un trafic bidirectionnel, sans interférer avec les autres flux de données, il aurait fallu appliquer le Default-VID 2 au port 5 afin que les données en provenance du port 5 appartiennent au VLAN 2. Cependant, il n'aurait plus accès au reste du réseau (identifié par le VLAN 1), à moins de modifier la configuration des autres switchs en modifiant l'appartenance de certains port au VLAN 2 (en plus du VLAN 1 par défaut).

*Dans le tableau de filtrage, bien identifier le point d'entrée (**N° de port - N° de VLAN**). La ligne du point d'entrée contient ainsi la liste de ports accessibles par les données émises depuis ce point.*

RÉGLER LA PRIORITÉ DES FLUX DE DONNÉES

Le switch HyperDSL permet de gérer les priorités des flux à 3 niveaux différents:

- **Physique (niveau 1)**: Permet l'attribution de 4 niveaux de priorités différents aux ports du switch. Il active une priorité générale d'un port par rapport aux autres en reservant les ressources (IntServ). Pour l'activer et le configurer, rendez-vous dans l'interface web, section « **Prioritization** » ou dans l'application Device Manager, **Menu Configuration > Editer > Configuration Harware.**

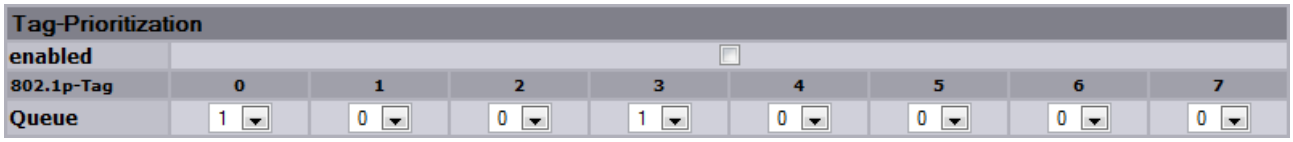
Port-Prioritization										
Port-Number	1	2	3	4	5	6	7	8	9	10
Queue	0	0	0	0	0	0	0	0	1	1

– **Liaisons de Données (niveau 2)**: Permet l'attribution de 4 niveaux de priorités différents aux trames Ethernet. Il existe initialement 8 degrés (norme 802.1P), mais le switch n'en gère que 4. Il faut donc réaliser l'association entre les différents niveaux via l'interface web.

Voici comment sont présentés ces niveaux:

Degrés	Type de trafic
7	Contrôle du réseau (network critical)
6	Voix interactive
5	Multimédia interactif
4	Application à charge controlé (streaming)
3	Service maximum (Business critical)
0	Service au mieux (Best effort)
2	Service économique (standard)
1	Arrière plan (background)

L'association avec les niveaux de priorités interne du switch se fait via l'interface web, section « **Prioritization** » et la mise en place des 8 degrés de priorités se fait lors de la configuration de VLAN (**Default-Priority**).



Il est aussi possible d'activer, mais pas d'éditer, ces niveaux de priorités dans l'application Device Manager: menu **Configuration > Editer > IEEE802.1p Gestion pritorités VLAN.**

– **Réseau (niveau 3)**: La méthode Differantiated Service (DiffServ) est de niveau Layer-3. Ici, on utilise les 6 premiers bites du champs Type of Service (ToS) de l'en-tête IP. Cela permet 64 Codepoints. On peut attribuer, pour chaque Codepoints, une priorité individuelle.

Vous pouvez accéder à la configuration de DiffServ via l'interface web, section « **Prioritization** », ou via l'application Device Manager, menu **Configuration > Editer > Ipv4/IPv6 Gestion priorités**.